Cybersecurity for Professionals
Comprehensive CompTIA Security+ Certification (SY0-601)

Course Tagline

Become a cybersecurity professional and CompTIA Security+ certified by hands-on learning of IT security, networking, cyber threats, attacks, vulnerabilities using Windows, Linux operating systems and other effective applications to pursue a skilled and successful career.

Course Highlights

- Blended learning delivery with 108 hours of instructor-led hybrid (onsite & online) training
- Certified & experienced trainers
- Hands on case studies where the candidates will use given tools and techniques
- Quiz to prepare for the CompTIA Security+ certificate examination
- CompTIA Security+ certificate examination fees reimbursement for successful candidates (a US$400 value)
- Internship opportunity after successful course completion
- Job support guidance

Course Overview

Cybersecurity is one of the most demandable job fields in this technology based modern world which is safeguarding of protected information and critical data online. Small to larger organizations implement cybersecurity measures to defend sensitive data from both internal and external threats and to best prepare for a cyber-attack.

The CompTIA Security+ certification validates that you have the core skills necessary for a career in the cybersecurity arena. It is a vendor-neutral security certification that is a good place to start. It teaches basic security concepts and is seen by many as the first port of call on the way to studying more advanced certifications. Because it is aimed at entry-level security professionals, it offers generalized information that will help candidates build a fundamental understanding of information security.

This comprehensive course is equivalent to two years of hands-on experience working in a security/systems administrator or specialist role. Candidates who will successfully complete this course will have the ability to pass the CompTIA Security+ certification exam.

Course Information

- Regular Class: Saturday and Sunday, 10 am – 2 pm | New York Time (EST)
- Review Class: Tuesday, 6.30 pm – 7.30 pm | New York Time (EST)
- Duration: 12 Weeks, 108 Hours
- Start Date and Course Fees:
  Please contact us to know the fees and updated batch schedule:
  https://qateksolutions.com/contact-us
- Textbook:
  CompTIA Security+ SY0-601 Certification Guide by Ian Neil.
  ISBN-13: 978-1800564244 | ISBN-10: 1800564244
- Target Audience
  - System Administrators
  - Security Engineers and consultants

- Network administrators
- IT Auditors/Penetration Testers

- Certificate exam (SY0-601) Information
  - Duration: 90 minutes
  - Number of questions: 90 questions per exam
  - Question format: Multiple choice and performance-based
  - Pass score: 750 (on a scale of 100-900)

Who Can Join?

The following are pre-requisites for this course:

- Bachelor's degree in any subject (Preferred but not required)
- Basic understanding of computing
- Anyone looking for a career change
- Proficiency in English will be a huge plus
- Must have a personal computer (desktop/laptop) with Microsoft Windows 2010/2011 or Apple macOS with good internet connection. The computer/laptop must have microphone, webcam, and Zoom software installed (we will help)

Learning Outcome

At the completion of the course, the candidates will be able to do the following:

- Assess the security posture of enterprise systems and information.
- Recommend and implement appropriate security solutions for different environments, including cloud, mobile, and IoT.
- Monitor security posture of enterprise systems and information
- Operate organizational systems with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents
- Prepare to sit for CompTIA Security+ certification examination: SY0-601

Instruction Method

- Live Instructor-led hybrid (onsite & online) training conducted in English

Tools to be used

- Microsoft Windows
- Linux OS (Ubuntu)
- Wireshark

Course Instructor (Mesbah Islam)

The lead instructor for CompTIA Security+ course is a veteran working in private and mostly in public sector as a software developer, Test Architect and Manager, and Cybersecurity professional. Currently he is performing the role of Information Security Manager in a highly visible federal agency. Our instructors have profound knowledge on market trend, demands, usability and hiring practices within public and private sector.

Course Outlines

Week 1 – Basic Computing: Computer Fundamentals, Operating Systems (OS)

- Computer architecture including hardware concepts and software introduction

- Internet, Email, Calendar Management, Remote Desktop, and VPN
- Video conferencing tools: Zoom, Meet, Teams
- Office communication tools: Slack
- Learning Management System (LMS)
- Operating Systems (OS): Microsoft Windows OS, Apple macOS, Linux OS (Ubuntu)
- Managing files, installing, and uninstalling software in different OS
- Graphical User Interface (GUI) intro in different OS
- Command Line Interface (CLI) examples in different OS

Week 2 – Basic Computing: Google Suite/Microsoft Office, Customer Service, Cybersecurity Basics

- Google Docs/MS Word
- Google Sheets/MS Excel
- Google Slides/MS PowerPoint
- Customer Service Principles, Problem Solving, Effective Communication
- Cybersecurity concepts, security threat with examples

Week 3 – Basic Networking

- Fundamental of Network
- Local Area Network (LAN) and Wide Area Network (WAN)
- Network layers
- Open System Interconnection (OSI) model
- Understanding of the OSI Layers

Week 4 – Basic Networking

- What is a port and the common network ports?
- Network protocol and how it works.
- What is a firewall
- Basics of routers and switches
- *Exam: Basic Computing & Networking and analysis of answers (Week 1-4)*

Week 5 – Threats, Attacks, and Vulnerabilities

- Compare and contrast different types of social engineering techniques
- Given a scenario, analyze potential indicators to determine the type of attacks.
- Explain different threat actors, vectors, and intelligence sources.

Week 6 – Threats, Attacks, and Vulnerabilities

- Explain the security concerns associated with various types of vulnerabilities
- Summarize the techniques used in security assessments
- Explain the techniques used in penetration testing

Week 7 – Architecture and Design

- Explain the importance of security concepts in an enterprise environment
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development, deployment, and automation concepts.
- Summarize authentication and authorization design concepts
- Given a scenario, implement cybersecurity resilience
- Explain the security implications of embedded and specialized systems.
- *Exam: Threats, Attacks, and Vulnerabilities and analysis of answers (Week 5-6)*

Week 8 – Architecture and Design | Implementation

- Explain the importance of physical security controls.
- Explain the basics of cryptographic concepts
- Given a scenario, implement secure protocols, and host or application security solutions,
- Given a scenario, implement secure network designs
- Given a scenario, install and configure wireless security settings.
- *Exam on Architecture and Design and analysis of answers (Week 7-8)*

Week 9 – Implementation

- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and account management controls
- Given a scenario, implement authentication and authorization solutions
- Given a scenario, implement public key infrastructure

Week 10 – Operations and Incident Response

- Given a scenario, use the appropriate tool to assess organizational security.
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation.
- Given an incident, apply mitigation techniques or controls to secure an environment.
- Explain the key aspects of digital forensics.
- *Exam on Implementation and analysis of answers (Week 9)*

Week 11 – Governance, Risk and Compliance

- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts
- Explain privacy and sensitive data concepts in relation to security.
- *Exam on Operations and Incident Response and analysis of answers (Week 10-11)*

Week 12 – Exam and Job Guidance

- Final Exam
- Job support guidance